BUNDESREPUBLIK DEUTSCHLAND

Bescheinigung

EPCC/2144
EJU

Die SCM Microsystems GmbH in Pfaffenhofen an der Ilm/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unauthorisierte Vervielfältigung"

am 18. März 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 11 B und G 06 F der Internationalen Patentklassifikation erhalten.

München, den 25. April 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Dzierzon

Aktenzeichen: 199 12 224.5

PRINZ & PARTNER GbR

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS
EUROPEAN TRADEMARK ATTORNEYS

Manzingerweg 7
D-81241 München
Tel. +49 89 89 69 80

18. März 1999

SCM Microsystems GmbH
Luitpoldstraße 6
85276 Pfaffenhofen

Unser Zeichen: S 4429 DE
HD/Hc

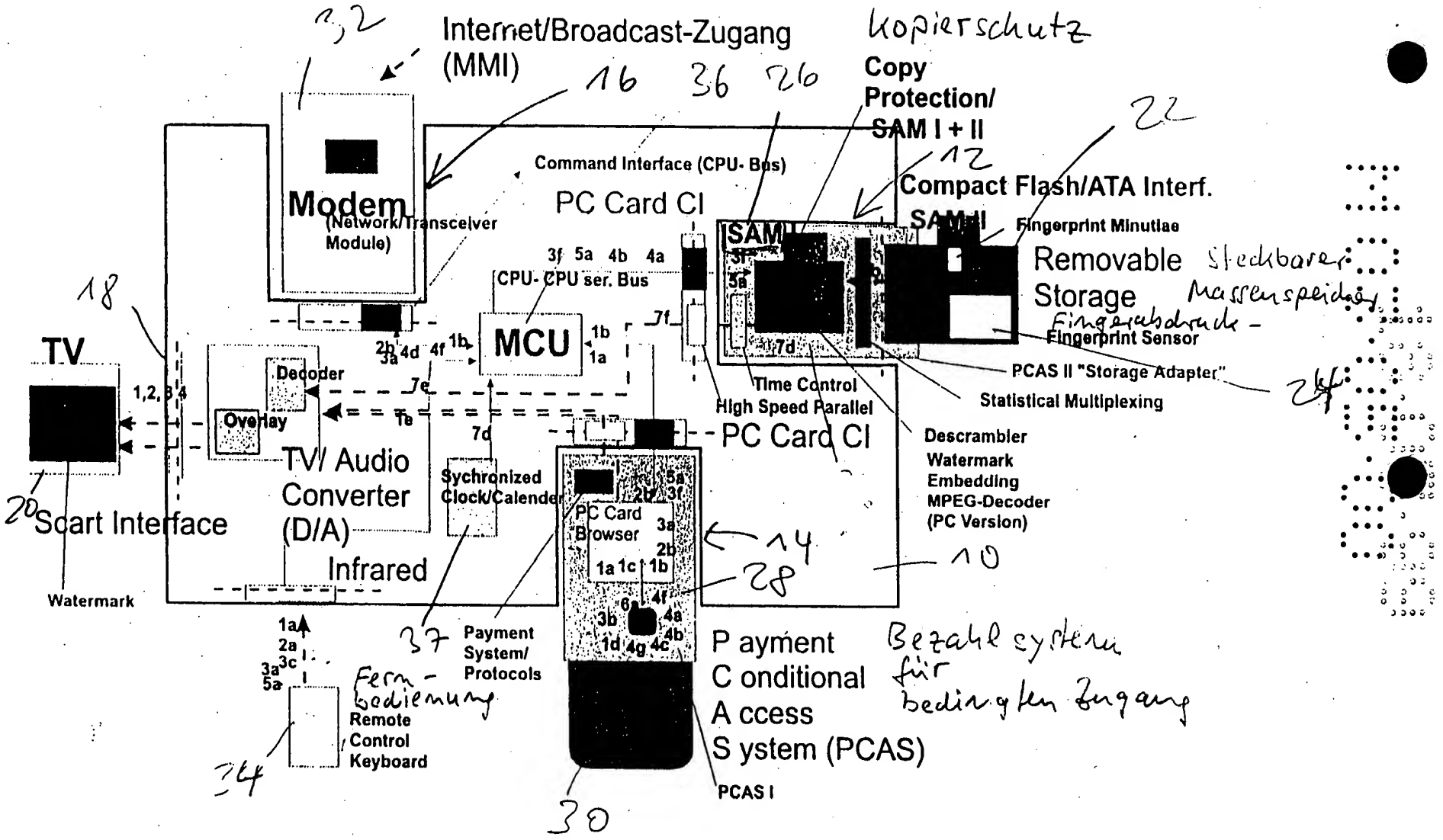
ZUSAMMENFASSUNG

Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unauthorisierte Vervielfältigung

---

Zur Sicherung von multimedialen Informationen und Software in einem tragbaren Massenspeicher gegen unauthorisierte Vervielfältigung werden die Daten in dem Massenspeicher in verzerrter Form gespeichert. In dem Wiedergabesystem für die Daten wird auf einem persönlichen SAM-Modul ein persönlicher Identitätscode des authorisierten Benutzers gespeichert. Die zur Entzerrung der Daten benötigten Entzerrungs-Schlüssel werden auf dem SAM-Modul des authorisierten Benutzers gespeichert. Den Daten wird ein Authorisierungs-Code zugeordnet, der auf dem SAM-Modul abgelegt wird. Auf dem SAM-Modul wird ein mittels des persönlichen Identitätscodes verschlüsselter Authorisierungscode gebildet und dann auf dem Massenspeicher abgelegt. Vor der Wiedergabe der Daten wird der verschlüsselte Authorisierungscode mittels des persönlichen Identitätscodes vom SAM-Modul entschlüsselt. Der entschlüsselte Authorisierungscode wird mit dem auf dem SAM-Modul abgelegten Authorisierungscode verglichen. Die Entzerrung der vom Massenspeicher ausgelesenen Daten mittels des Entzerrungsschlüssels wird nur bei übereinstimmenden Authorisierungscodes freigegeben.

Fig. 1


Internet/Broadcast-Zugang
(MMI)
Kopierschutz
Copy
Protection/
SAM I + II
Command Interface (CPU- Bus)
Modem
(Network/Transceiver
Module)
PC Card CI
Compact Flash/ATA Interf.
SAM I
SAM II
Fingerprint Minutiae
Removable
Storage
Steckbarer
Massenspeicher
Fingerabdruck-
Fingerprint Sensor
CPU- CPU ser. Bus
MCU
TV
Decoder
Overlay
TV/ Audio
Converter
(D/A)
Infrared
Scart Interface
Watermark
Sychronized
Clock/Calender
Time Control
High Speed Parallel
PCAS II "Storage Adapter"
Statistical Multiplexing
Descrambler
Watermark
Embedding
MPEG-Decoder
(PC Version)
PC Card CI
PC Card
Browser
Payment
System/
Protocols
Fern-
bedienung
Remote
Control
Keyboard
P ayment
C onditional
A ccess
S ystem (PCAS)
Bezahlsystem
für
bedingten Zugang
PCAS I

PRINZ & PARTNER GbR

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS
EUROPEAN TRADEMARK ATTORNEYS

Manzingerweg 7
D-81241 München
Tel. +49 89 89 69 80

18. März 1999

SCM Microsystems GmbH
Luitpoldstraße 6
85276 Pfaffenhofen

Unser Zeichen: S 4429 DE
HD/Hc

Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unauthorisierte Vervielfältigung

---

Die Erfindung betrifft ein Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unauthorisierte Verfielfältigung und ein Wiedergabesystem zur Durchführung des Verfahrens.

Die kommerzielle Verbreitung von multimedialen Inhalten und Software geschieht ganz überwiegend auf Datenträgern, die nur einmal beschreibbar sind und mit dem darauf gespeicherten Inhalt das Handelsprodukt bilden. Die kommerzielle Verbreitung der Inhalte losgelöst von solchen Datenträgern wäre prinzipiell möglich, beispielsweise durch Fernzugriff auf Netzwerke mit Bezahlfunktion, scheitert jedoch am mangelnden Schutz gegen unauthorisierte Verfielfältigung.

Durch die Erfindung wird ein Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unauthorisierte Verfielfältigung zur Verfügung gestellt, das mit geringem Aufwand und verfügbarer Technologie durchgeführt werden kann. Nach dem erfindungsgemäßen Verfahren werden die Daten in dem Massenspeicher zunächst in verzerrter Form gespeichert. In

einem Wiedergabesystem für die Daten wird wenigstens ein SAM-Modul (Safe Access Modul, d.h. Modul für gesicherten Zugriff) verwendet, auf dem ein persönlicher Identitätscode eines authorisierten Benutzers gespeichert ist. Die zur Entzerrung der Daten benötigten Entzerrungs-Schlüssel werden auf dem SAM-Modul des authorisierten Benutzers gespeichert. Den Daten wird ein Authorisierungscode zugeordnet, der auf dem SAM-Modul abgelegt wird. Auf dem SAM-Modul wird sodann ein mittels des persönlichen Identitätscodes verschlüsselter Authorisierungscode gebildet. Dieser verschlüsselte Authorisierungscode wird mit den verzerrten Daten auf dem Massenspeicher abgelegt. Vor einer Wiedergabe der Daten wird der verschlüsselte Authorisierungscode mittels des persönlichen Identitätscode vom SAM-Modul entschlüsselt. Der entschlüsselte Authorisierungscode wird dann mit dem auf dem SAM-Modul (unverschlüsselt) abgelegten Authorisierungscode verglichen. Die Entzerrung der vom Massenspeicher ausgelesenen Daten mittels der Entzerrungsschlüssel wird dann nur bei übereinstimmenden Authorisierungscodes freigegeben. Durch dieses mit einfachster Hardware durchführbare Verfahren erfolgt eine Personalisierung der Daten auf dem Massenspeicher. Für die unverzerrte Wiedergabe der Daten wird ein Authorisierungscode benötigt, der nur über den SAM-Modul des authorisierten Benutzers gewonnen werden kann, weil er mit dem persönlichen Identitätscode des authorisierten Benutzers verknüpft ist.

In Weiterbildung des Verfahrens werden auch die für die Entzerrung der Daten benötigten Entzerrungsschlüssel mit auf dem SAM-Modul gespeicherten persönlichen Daten des authorisierten Benutzers chiffriert, so daß sie nur unter Verwendung des zutreffenden SAM-Moduls dechiffriert werden können.

In weiterer Ausgestaltung des Verfahrens werden die Daten bei der Wiedergabe über ein geeignetes Wiedergabesystem unlösbar mit einer persönlichen Kennzeichnung des authorisierten Benutzers ausgegeben. Die persönliche Kennzeichnung kann in einem Logo oder dergleichen bestehen, das bei Bilddaten in einer Ecke des Bildfeldes angezeigt wird.

Das erfindungsgemäße Wiedergabesystem zur Durchführung des Verfahrens enthält im wesentlichen: Ein Lesemodul zur Aufnahme des Massenspeichers, bei dem es sich vorzugsweise um ein vom Anwender beschreibbares Medium handelt, beispielsweise eine miniaturisierte Festplatte oder eine vom

Benutzer beschreibbare optische Speicherplatte; einen Kartenleser für das SAM-Modul; eine Daten-Aufbereitungselektronik zum Entzerren der aus dem Massenspeicher gelesenen Daten; und ein Ausgabegerät für die entzerrten Daten. Um Daten über ein entferntes Netzwerk, beispielsweise aus dem Internet, beziehen zu können, ist vorzugsweise zusätzlich ein Bezahlsystem für den bedingten Zugang zu einem Datenanbieter über das entfernte Netzwerk vorgesehen. Das Bezahlsystem basiert auf einem Chipkartenleser, der bei der bevorzugten Ausführungsform als steckbare PC-Karte im PCMCIA-Format ausgebildet ist.

Weitere Vorteile und Merkmale der Erfindung ergeben sich aus der folgenden Beschreibung und aus der Zeichnung, auf die Bezug genommen wird. In der Zeichnung zeigen:

Das in Figur 1 gezeigte Blockschaltbild eines Wiedergabesystems zur Durchführung des erfindungsgemäßen Verfahrens zeigt schematisch die wesentlichen Komponenten des Systems. Eine in einem kompakten Gehäuse untergebrachte Schnittstelleneinrichtung ist allgemein mit 10 bezeichnet und weist drei Schnittstellen 12, 14, 16 für steckbare Komponenten sowie einen Ausgangsanschluß 18 für ein Video-Ausgabegerät 20 auf. Die Schnittstelle 12 hat einen Stecksockel für einen Massenspeicher 22, der auf einer dem Benutzer zugänglichen Fläche einen Fingerabdruck-Sensor 24 aufweist. Ein erstes SAM-Modul 26 ist Bestandteil der Schnittstelle 12. Ein zweites SAM-Modul ist in dem steckbaren Massenspeicher 22 enthalten. Dieser Massenspeicher kann eine miniaturisierte Festplatte oder auch ein Halbleiterspeicher sein, beispielsweise in FLASH-Techologie.

Die Schnittstelle 14 nimmt einen Chipkartenleser 28 im Format einer PC-Karte (Abkürzung für PCMCIA-Karte) auf. Der Chipkartenleser 28 bildet in Verbindung mit einer Chipkarte 30, auch als Smart Card bezeichnet, ein Bezahlsystem für den bedingten Zugang zu einem Anbieter multimedialer Inhalte und dergleichen, insbesondere über das Internet.

An der Schnittstelle 16 wird ein Modem 32 oder ein Netzwerkadapter angeschlossen. Über das Modem 32 oder den Netzwerkadapter kann der Zugriff auf ein entferntes Netzwerk, insbesondere das Internet, erfolgen.

Am Ausgangsanschluß 18, der als SCART-Schnittstelle ausgeführt sein

kann, wird ein Fernsehempfänger oder Monitor angeschlossen.

Das Wiedergabesystem kann ferner mit einer Infrarot-Fernbedienung 34 ausgestattet sein.

Ein interner Prozessor 36 beinhaltet die notwendige Funktionalität zur Entzerrung und Aufbereitung der von dem Massenspeicher 22 ausgelesenen Daten für die Wiedergabe auf dem Ausgabegerät 20. Der Prozessor 36 ist mit einem synchronisierten Zeitgeber 37 gekoppelt, der Bestandteil einer Überwachungseinrichtung ist, mittels welcher die Aufbereitung der Daten zur Wiedergabe von einem zertifizierten Zeitstempel abhängig gemacht wird, der mit den Daten auf dem Massenspeicher 22 aufgezeichnet ist.

Das erfindungsgemäße Verfahren ist in den Diagrammen der Figuren 2, 3 und 4 dargestellt. Es besteht im wesentlichen aus drei Stufen. In der ersten, in Figur 2 dargestellten Stufe des Verfahrens erfolgt eine Personalisierung der Daten im Massenspeicher. Der Vorgang wird mit der Übersendung eines System-Zertifikats zum Anbieter der Daten begonnen. Bei den Daten handelt es sich insbesondere um multimediale Informationen, abgekürzt als MMI. Durch das Systemzertifikat weist sich das Wiedergabesystem beim MMI-Anbieter als geeignetes System aus. Seitens des MMI-Anbieters wird dann aus dem SAM-Modul des Wiedergabesystems ein privater Schlüssel empfangen, um einen Wiedergabe-Authorisierungscode zu erzeugen. Bei dem privaten Schlüssel kann es sich um einen persönlichen Identitätscode oder auch um vom Fingerabdruck-Sensor 24 abgeleitete komprimierte Daten, oder eine Kombination derselben, handeln. Der Wiedergabe-Authorisierungscode wird dann auf dem SAM-Modul gespeichert.

Anschließend erfolgt mittels des Bezahlsystems 28, 30, die Bezahlung, woraufhin die MMI-Daten in verzerrter Form heruntergeladen und auf dem MMI-Massenspeicher 22 gespeichert werden. Anschließend werden die zur Entzerrung der MMI-Daten benötigten MMI-Schlüssel in chiffrierter Form zum SAM-Modul übertragen und dort gespeichert. Ferner wird vom MMI-Anbieter ein chiffriertes Wasserzeichen gesendet, das im SAM-Modul gespeichert werden kann, wenn der Umfang der entsprechenden Daten vergleichsweise gering ist; andernfalls erfolgt die Speicherung im Massenspeicher. Optional wird mit den MMI-Daten ein zertifizierter Zeitstempel gesendet und auf dem Massenspeicher 22 aufgezeichnet.

Als letzter Schritt der ersten Verfahrensstufe wird vom MMI-Anbieter ein chiffrierter Authorisierungscode gesendet, der im MMI-Massenspeicher zusammen mit den MMI-Daten gespeichert wird.

Wenn in den privaten Schlüssel die durch den Fingerabdruck-Sensor abgegebenen Daten eingehen, können diese durch den im Massenspeicher 22 integrierten SAM-Modul ver- oder bearbeitet werden.

Die in Figur 3 gezeigte Verfahrensstufe betrifft die Überprüfung der Wiedergabe-Authorisierung. In dem SAM-Modul wird dazu der aus dem Massenspeicher gelesene chiffrierte Authorisierungscode mittels des privaten Schlüssels dechiffriert; der so zurückgewonnene Authorisierungscode wird dann mit dem auf dem SAM-Modul gespeicherten Authorisierungscode verglichen. Bei übereinstimmenden Authorisierungscodes wird der Wiedergabeprozeß freigegeben.

Bei dem in Figur 4 gezeigten Wiedergabe-Prozeß wird zunächst im SAM-Modul der MMI-Schlüssel mittels des privaten Schlüssels dechiffriert. Dann werden die MMI-Daten aus dem Massenspeicher ausgelesen und mittels des dechiffrierten MMI-Schlüssels entzerrt. Die entzerrten MMI-Daten werden dann mit dem persönlichen Logo bzw. Wasserzeichen überlagert und an das Ausgabegerät abgegeben.

Durch den optional mit den MMI-Daten aufgezeichneten zertifizierten Zeitstempel kann die zugelassene Wiedergabe der Daten zeitlich befristet werden.

PRINZ & PARTNER GbR

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS
EUROPEAN TRADEMARK ATTORNEYS

Manzingerweg 7
D-81241 München
Tel. +49 89 89 69 80

18. März 1999

SCM Microsystems GmbH
Luitpoldstraße 6
85276 Pfaffenhofen

Unser Zeichen: S 4429 DE
HD/Hc

Patentansprüche

1. Verfahren zur Sicherung von Daten in einem tragbaren Massenspeicher gegen unauthorisierte Vervielfältigung, insbesondere zum Schutz von multimedialen Informationen und Software, dadurch gekennzeichnet, daß:

a) die Daten in dem Massenspeicher in verzerrter Form gespeichert werden;

b) in einem Wiedergabesystem für die Daten wenigstens ein persönlicher SAM-Modul verwendet wird, auf dem ein persönlicher Identitätscode des authorisierten Benutzers gespeichert ist;

c) wenigstens ein zur Entzerrung der Daten benötigter Entzerrungs-Schlüssel auf dem SAM-Modul des authorisierten Benutzers gespeichert wird;

d) den Daten ein Authorisierungs-Code zugeordnet wird, der auf dem SAM-Modul abgelegt wird;

e) auf dem SAM-Modul ein mittels des persönlichen Identitätscodes verschlüsselter Authorisierungscode gebildet wird;

f) der verschlüsselte Authorisierungscode auf dem Massenspeicher abgelegt wird;

g) vor einer Wiedergabe der Daten der verschlüsselte Authorisierungscode mittels des persönlichen Identitätscodes vom SAM-Modul entschlüsselt wird;

h) der entschlüsselte Authorisierungscode mit dem auf dem SAM-Modul abgelegten Authorisierungscode verglichen wird und die Entzerrung der vom Massenspeicher ausgelesenen Daten mittels des Entzerrungsschlüssels nur bei übereinstimmenden Authorisierungscodes freigegeben wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß vor dem Erwerb der Daten von einem Anbieter ein System-Zertifikat vom SAM-Modul zum Anbieter gesendet und von diesem überprüft wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß für die gesicherte Übertragung des Authorisierungscodes zum SAM-Modul des authorisierten Benutzers ein Sitzungs-Schlüssel verwendet wird.

4. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß zur Personalisierung der Daten auf dem Massenspeicher eine Kennzeichnung aus persönlichen Merkmalen des authorisierten Benutzers gebildet und mit den Daten is solcher Weise verknüpft wird, daß die Daten nur mit der Kennzeichnung ausgegeben werden können.

5. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der persönliche Identitätscode des authorisierten Benutzers zumindest teilweise aus von einem Fingerabdruck-Sensor gelieferten Daten gebildet wird.

6. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Massenspeicher in einem an einem Wiedergabesystem steckbaren Modul angeordnet ist.

7. Verfahren nach den Ansprüchen 5 und 6, dadurch gekennzeichnet, daß der Fingerabdruck-Sensor auf einer Fläche des steckbaren Moduls angeordnet ist.

8. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß mittels eines ersten, im Wiedergabesystem angeordneten SAM-Moduls die Kommunikation und Transaktion mit dem Anbieter der Daten und mittels eines zweiten, dem Massenspeicher zugeordneten SAM-Moduls die Personalisierung der Daten abgewickelt werden.

9. Verfahren nach den Ansprüchen 6 und 8, dadurch gekennzeichnet, daß das dem Massenspeicher zugeordnete SAM-Modul in das steckbare Modul integriert ist.

10. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Massenspeicher als miniaturisierte Festplatte ausgebildet ist.

11. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß der Massenspeicher als Flash-Halbleiterspeicher ausgebildet ist.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß der Flash-Halbleiterspeicher entfernbar in einem am Wiedergabesystem steckbaren Schnittstellen-Modul angeordnet ist.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß das Schnittstellen-Modul einen SAM-Kartenleser enthält.

14. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß zum Erwerb der Daten eine Kommunikation und Transaktion mit einem Anbieter per Fernzugriff auf ein Netzwerk erfolgt.

15. Verfahren nach Anspruch 14, dadurch gekennzeichnet, daß die Transaktion mit dem Anbieter unter Verwendung eines in das Wiedergabesystem einsteckbaren Kartenleser-Moduls erfolgt, das einen Chip-

Kartenleser und einen das wenigstens eine SAM-Modul aufnehmenden SAM-Kartenleser beinhaltet.

16. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Entzerrungsschlüssel seinerseits mit auf dem SAM-Modul gespeicherten persönlichen Daten chiffriert und bei der Wiedergabe mit diesen Daten dechiffriert wird.

17. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß ein zertifizierter Zeitstempel erzeugt und mit den Daten auf dem Massenspeicher gespeichert wird.

18. Wiedergabesystem zur Durchführung des Verfahrens nach einem der vorstehenden Ansprüche, gekennzeichnet durch:

- ein Lesemudul zur Aufnahme des Massenspeichers;
- einen Kartenleser für das SAM-Modul;
- eine Daten-Aufbereitungselektronik zum Entzerren der aus dem Massenspeicher gelesenen Daten; und
- ein Ausgabegerät für die entzerrten Daten.

19. Wiedergabesystem nach Anspruch 16, ferner gekennzeichnet durch ein auf einem Chipkartenleser basierendes Bezahlsystem für bedingten Zugang zu einem Datenanbieter über ein entferntes Netzwerk.

20. Wiedergabesystem nach Anspruch 17, dadurch gekennzeichnet, daß der Chipkartenleser als steckbare PC-Karte im PCMCIA-Format ausgebildet ist.

21. Wiedergabesystem nach einem der Ansprüche 18 bis 20, dadurch gekennzeichnet, daß eine Überwachungseinrichtung vorgesehen ist, die einen mit den Daten vom Massenspeicher gelesenen zertifizierten Zeitstempel auswertet.

Fig. 1

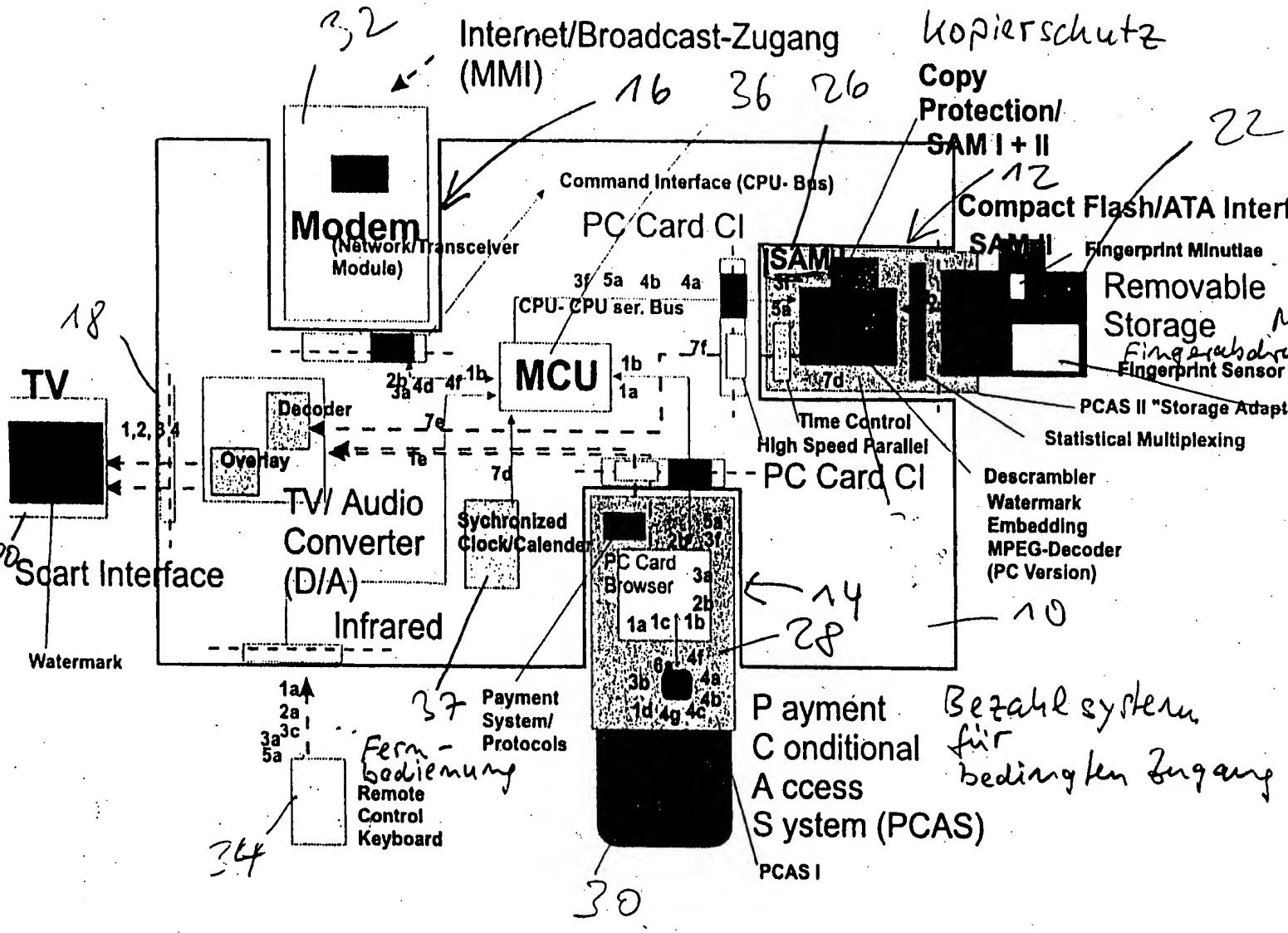


Fig. 2 Personalisierung MMI-Massenspeicher

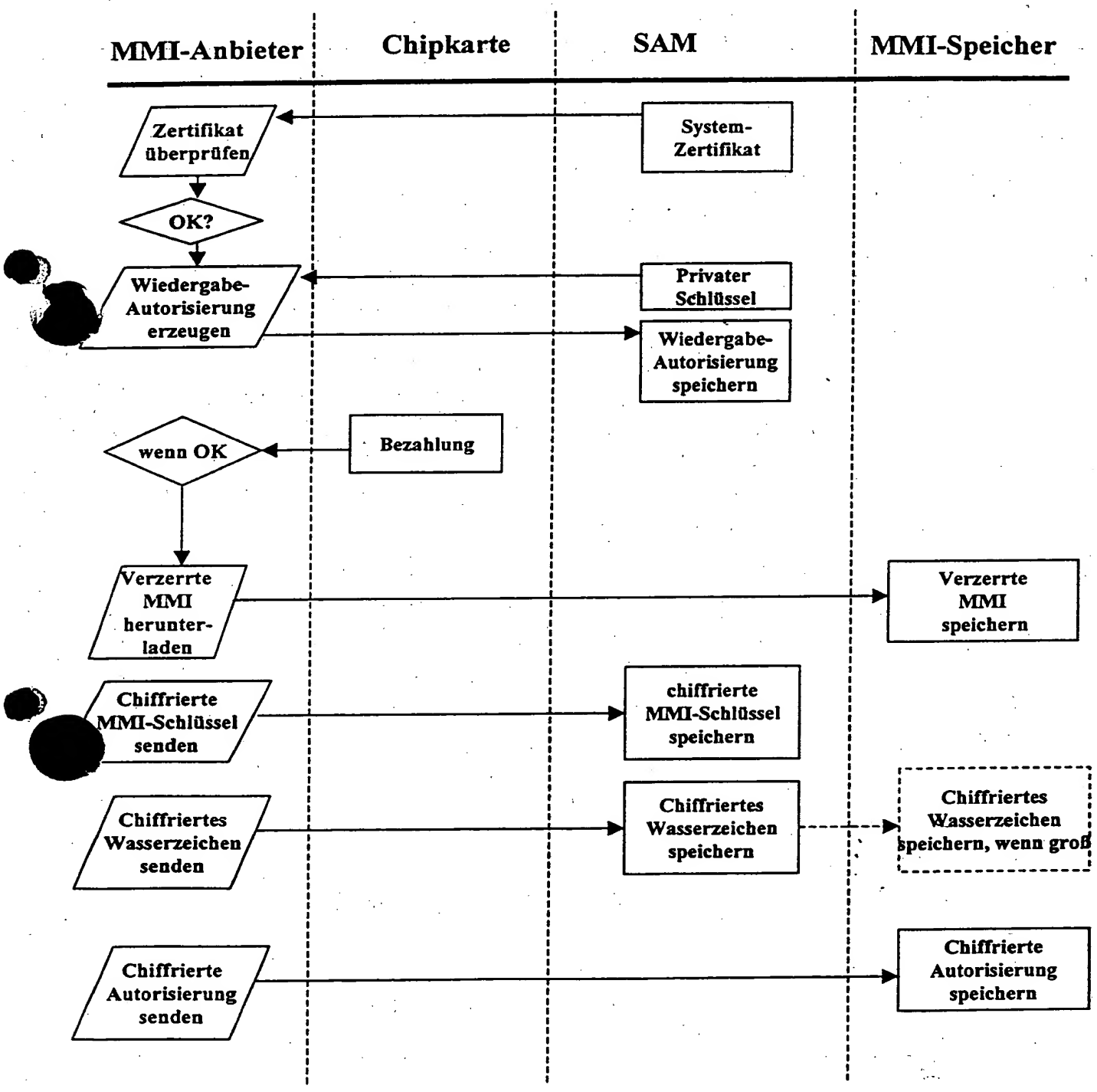


Fig. 3 Überprüfung Wiedergabe-Autorisierung

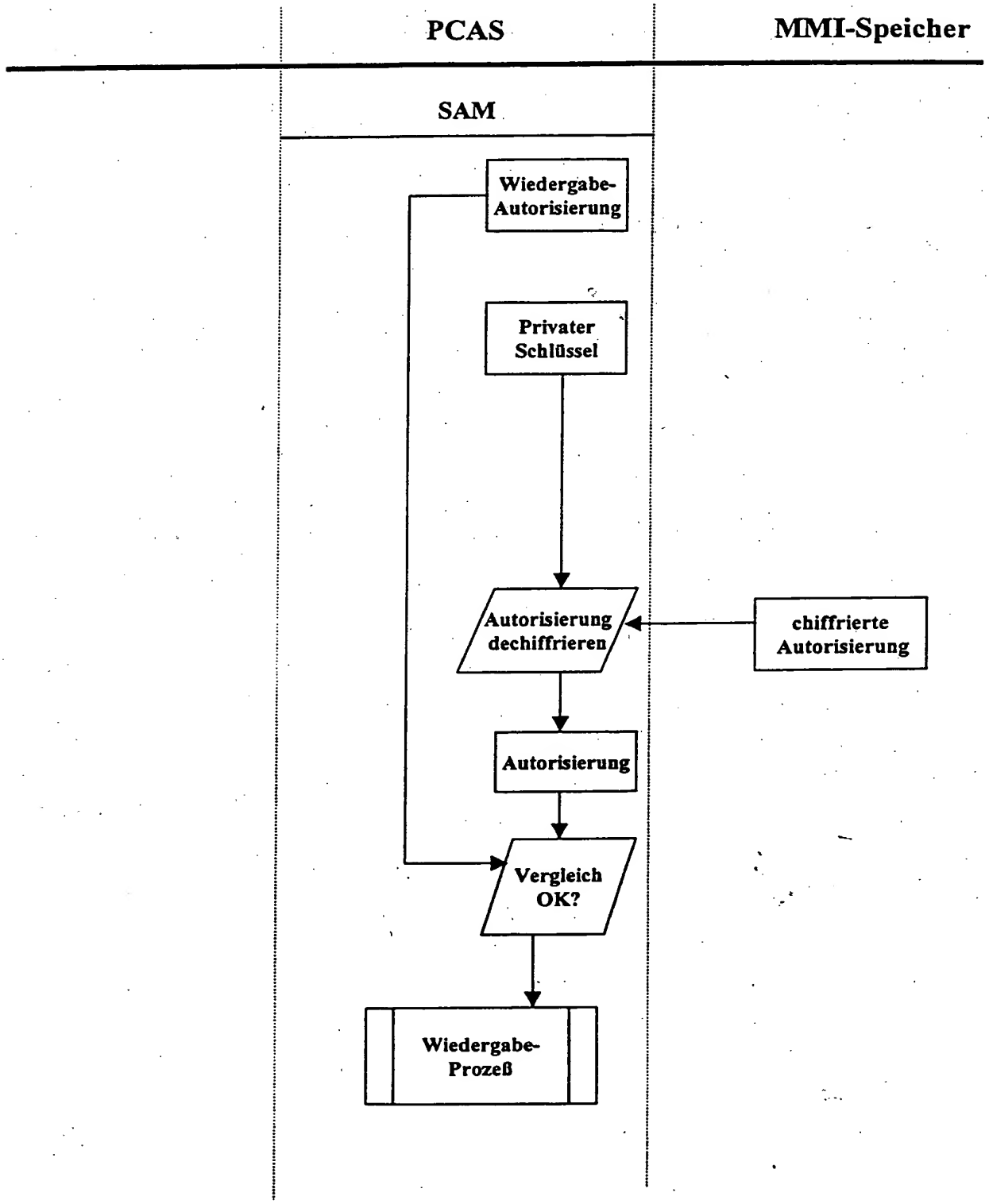


Fig. 4 Wiedergabe-Prozeß